ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2012
Seria: ORGANIZACJA I ZARZĄDZANIE z. 61 Nr kol. 1873

Andrzej MICHALSKI
Politechnika Śląska
Wydział Organizacji i Zarządzania
Instytut Ekonomii i Informatyki
Zakład Informatyki i Ekonometrii

BEZPIECZEŃSTWO INFORMACJI W PRZYPADKU AWARII LUB KATASTROFY

Streszczenie. Dla współczesnej organizacji gospodarczej posiadane zasoby informacyjne stanowią jeden z najważniejszych czynników zapewnienia realizacji procesów biznesowych. Utrata danych w wyniku awarii systemu lub zaistniałej katastrofy najczęściej uniemożliwia powrót do prawidłowego funkcjonowania na rynku. W artykule przeanalizowano potencjalne przyczyny utraty informacji i omówiono sposoby zapobiegania utracie danych i sposoby ich odtwarzania w przypadku katastrofy.

INFORMATION SECURITY IN THE CASE OF DISASTER OR SYSTEM MALFUNCTION

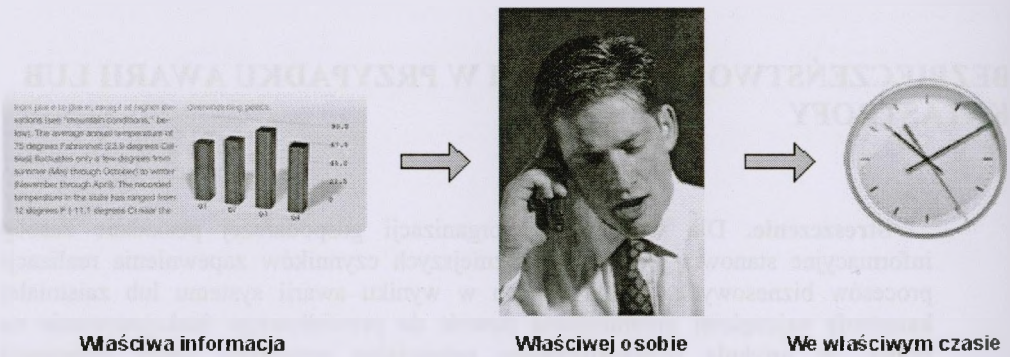
Summary. In the contemporary enterprise all business processes can be carried out mainly thanks to company's information resources. Data loss in the case of disaster or system malfunction often results in disappearing the company from the market. In the paper possible causes of such scenario and methods how to prevent data loss and recover the system after disaster are presented.

1. Wprowadzenie

Zwiększający się udział informacji jako składnika kosztów produktu finalnego oraz duża dynamika procesów produkcyjnych stanowią obiektywne przesłanki, determinujące konieczność wykorzystania w działalności przedsiębiorstwa systemu informatycznego

zarządzania, ponieważ związane z tym przetwarzanie znacznych ilości informacji jest możliwe do osiągnięcia jedynie przez wspomaganie komputerowe. Równocześnie stały rozwój technologii informatycznych udostępnia środki do realizacji tych celów [19].

System informatyczny organizacji, jak każda inwestycja, powinien być elementem zwiększania zysków przez wspomaganie procesu decyzyjnego. Podstawowy cel funkcjonalny systemu można przedstawić w postaci sformułowania: dostarczenie właściwej informacji właściwej osobie we właściwym czasie (rys. 1), co przekłada się na dostępność informacji w czasie określonym przez procesy biznesowe [19].



Rys. 1. Podstawowa funkcja systemu informatycznego – dostarczanie informacji [19]
Fig. 1. The main function of information system – information delivery [19]

W takim przypadku podstawą działań biznesowych stają się przepływ i wykorzystanie informacji, a zasoby informacyjne przedsiębiorstwa nabierają pierwszorzędnego znaczenia.

2. Zagrożenia związane z awariami i katastrofami

Problemy związane z bezpieczeństwem informacji i zapewnieniem wysokiego poziomu jej dostępności dotyczą przypadków, w których pojawia się sytuacja awaryjna, wywołana niesprawnością systemu.

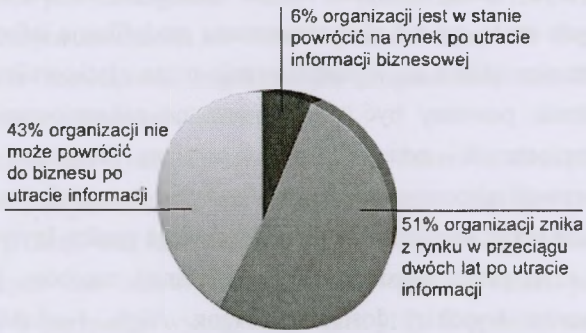
Przyjęło się rozgraniczać dwa typy stanu braku lub ograniczenia dostępności do zasobów systemowych [18], [20]:

- awaria, kiedy uszkodzeniu ulega niewielki fragment systemu (w zakresie zasobów sprzętowych lub programowych lub obu tych obszarów równocześnie), a do przywrócenia pełnej sprawności systemu wystarczają działania natury serwisowej;
- katastrofa, gdy uszkodzeniu lub całkowitemu zniszczeniu ulega większość istniejącej infrastruktury systemowej, a do przywrócenia sprawności systemu niezbędne są

działania związane z odtwarzaniem zniszczonych zasobów sprzętowych, nieruchomości, danych i często zasobów ludzkich (rys. 2).

Rys. 2. Zniszczenia infrastruktury w wyniku katastrofy [23]
Fig. 2. Infrastructure destroyed after disaster [23]

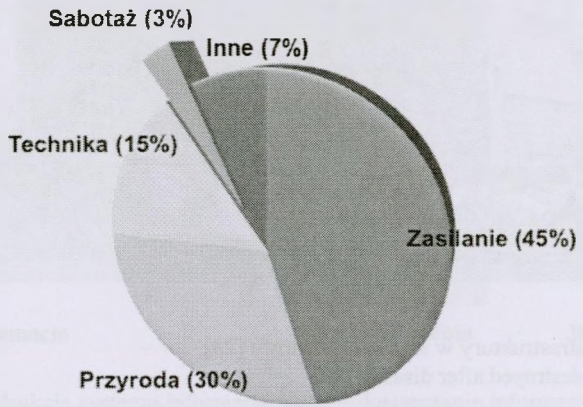
Bezpieczeństwo posiadanej i wymienianej informacji ma bezpośredni wpływ na realizację celu organizacji, w tym na: osiąganie przychodu z prowadzonej działalności, zachowanie płynności finansowej oraz kreowanie pozytywnego wizerunku marketingowego (pozycji na rynku) [4].



Rys. 3. Przedsiębiorstwa po utracie zasobów informacyjnych (opracowanie własne na podstawie [28])
Fig. 3. Enterprises after data loss (author's own based on [28])

Przeprowadzone badania [28] wskazują, że w przypadku utraty przez organizację swoich zasobów informacyjnych (np. w wyniku katastrofy) powrót przedsiębiorstwa do normalnych relacji rynkowych jest bardzo mało prawdopodobny – tylko ok. 6% takich przedsiębiorstw powraca do normalnego funkcjonowania (rys. 3).

Jest wiele czynników, które mogą doprowadzić do utraty danych. Zwykle są one grupowane w klasy zagrożeń. Na rys. 4 przedstawiono wyniki wieloletnich badań firmy APC w tym zakresie [2], [19], a mianowicie procentowy układ tych klas zagrożeń w ogólnej liczbie przypadków narażenia na utratę danych organizacji.



Rys. 4. Podstawowe przyczyny utraty danych (opracowanie własne na podstawie [2])
Fig. 4. Main causes of data loss (author's own based on [2])

Analizując przyczyny utraty danych, można zauważyć, że bezwzględna większość zdarzeń powodujących utratę czy też nieautoryzowaną modyfikację informacji ma charakter obiektywny, tzn. jest niemożliwa do wyeliminowania przez użytkownika systemu. A zatem podejmowane działania powinny być nakierowane na zabezpieczenie przed skutkami wystąpienia niebezpiecznych sytuacji, czyli powinny zmierzać do zapewnienia bezpieczeństwa informacji mimo wystąpienia awarii czy też katastrofy (rys. 5).

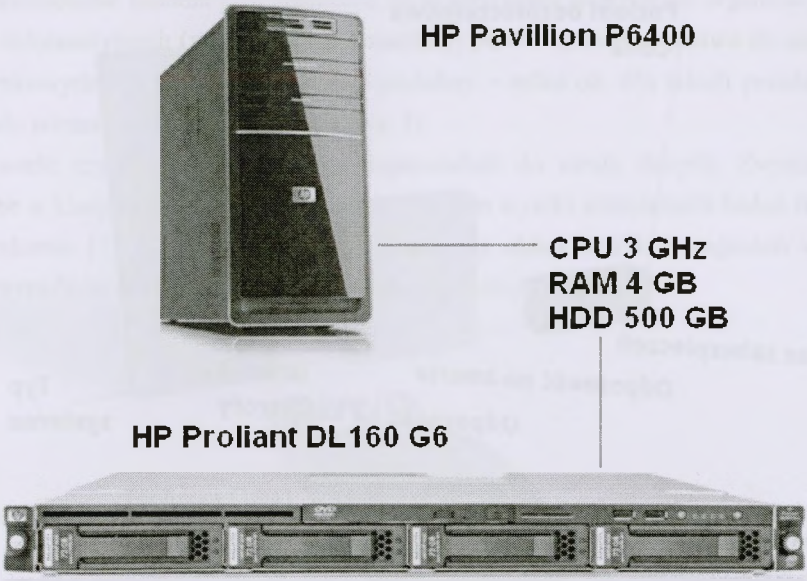
Jest to realizowane przez wyeliminowanie pojedynczego punktu krytycznego (ang. *Single Point of Failure*), czyli przez wprowadzenie redundancji zasobów, jak to ma miejsce w przypadku serwerów wysokiej dostępności (ang. *High Availability Servers*), oraz wprowadzenie odporności na katastrofy (ang. *Disaster Tolerance*).

Rys. 5. Poziomy ochrony systemu informatycznego przed utratą informacji w relacji do ceny (opracowanie własne)
Fig. 5. The levels of the information system security vs. price (author's own)

3. Serwery wysokiej dostępności

Nie jest możliwe stworzenie komputerów, które w ogóle nie będą się psuły, w których nie wystąpią awarie. Jednakże możliwe jest takie zaprojektowanie komputera, że mimo wystąpienia awarii jednego lub kilku podzespołów komputer będzie mógł zapewnić dostarczanie niezbędnej mocy obliczeniowej w sposób nieprzerwany [15], [17]. Taki rodzaj wysokiej dostępności jest szczególnie ważny w przypadku przetwarzania dużych ilości informacji o krytycznym znaczeniu, co obecnie jest sytuacją dość częstą [3]. Oczywiście wymagane są także rozwiązania organizacyjno-programowe, umożliwiające skuteczne zarządzanie środkami przetwarzania informacji [14].

Wysoka dostępność jest wymagana zwłaszcza od serwerów, niezależnie od tego, czy są one wykorzystywane jako urządzenia samodzielne, elementy klastrów (ang. *clusters*) czy też farm serwerów [1]. Stąd też konstruktorzy wyposażają współczesne serwery w wiele rozwiązań bazujących na nowoczesnych technologiach, które pozwalają zapewnić nieprzerwaną pracę w przypadku wystąpienia awarii [16]. U podstaw takich rozwiązań leży koncepcja redundancji (nadmiarowości zasobów), dzięki której uszkodzenie określonego podzespołu nie wpływa na poziom dostępności mocy obliczeniowej, dostarczanej przez serwer [9], [22]. Równocześnie wysoki poziom dostępności ma bezpośredni wpływ na cenę urządzenia (rys. 6).



Rys. 6. Dwa komputery o takiej samej wydajności, różniące się ceną o rząd wielkości (cena górnego to 2500 zł, cena dolnego to 25 000 zł; opracowanie własne na podstawie ofert firmy Hewlett-Packard na witrynie www.hp.pl, luty 2011)

Fig. 6. Two computers with the same computational power but different price tags (Pavillion's price is 2500 zł while Proliant's price is 25 000 zł; author's own based on the Hewlett-Packard company's site offers, available on www.hp.pl, February 2011)

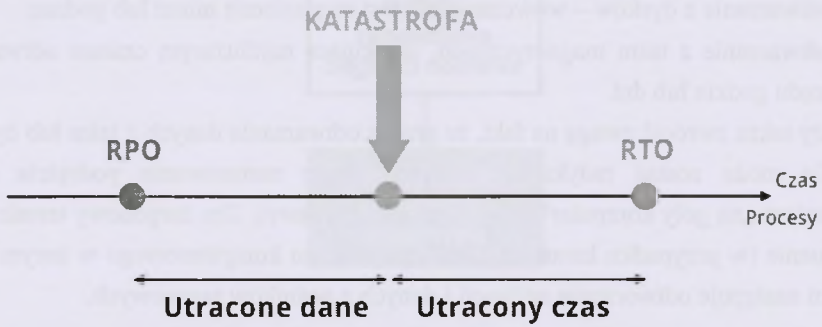
Redundancja obejmuje wszystkie obszary krytyczne, a mianowicie:

- zasilanie;
- przetwarzanie i kontrolę danych;
- przechowywanie informacji;
- komunikację ze światem zewnętrznym;
- zarządzanie systemem i działania serwisowe.

Dzięki temu poziom dostępności wzrasta z ok. 99%, jak to ma miejsce w przypadku komputerów ogólnego przeznaczenia (co odpowiada ok. 4 dniom przestoju w ciągu roku), do 99,99999% w przypadku serwerów do zastosowań krytycznych (co jest równoważne kilku minutom przestoju w ciągu roku).

4. Odporność na skutki awarii

Katastrofa może być zdefiniowana jako niezaplanowane wydarzenie, które w istotny sposób dotyka działań biznesowych przedsiębiorstwa i jest związane z ryzykiem bankructwa firmy w wyniku: utraty rynku, narażenia na procesy sądowe lub utraty zysków. Skutki katastrofy rozciągają się znacznie poza utratę (nawet skopiowanych) danych – zwykle dotyczą zniszczeń budynku, instalacji i/lub zniszczeń systemu komputerowego. Ma to miejsce zarówno w przypadku naturalnego kataklizmu, jak i działań ludzkich, jak np. atak terrorystyczny, zainfekowanie wirusem komputerowym czy też zablokowanie systemu [24]. Dwa najważniejsze parametry z punktu widzenia zarządzania zasobami informacyjnymi, przedstawione na rys. 7, to czas odtwarzania (ang. *Recovery Time Objective – RTO*) i punkt odtwarzania (ang. *Recovery Point Objective – RPO*) [11].



Rys. 7. Katastrofa i odtwarzanie systemu (opracowanie własne na podstawie [11] i [20])
Fig. 7. System disaster and disaster recovery (author's own based on [11] and [20])

Punkt odtwarzania (RPO) określa następujący element: „Na jak dużą utratę danych może sobie pozwolić użytkownik?" Punkt ten to moment z przeszłości, w którym po raz ostatni została wykonana kopia danych i do którego momentu naszej działalności będziemy mogli wrócić (np. po awarii). Parametr ten dla różnych firm może mieć inną wartość – jednym wystarczy kopia sprzed tygodnia, inni zaś potrzebują danych sprzed kilkunastu sekund [8]. Czas odtwarzania (RTO) odpowiada z kolei na pytanie: „Jak długo użytkownik może oczekiwać na ponownie dostępne dane i funkcje organizacji gospodarczej?" Czas ten jest maksymalnym czasem po katastrofie, który jest niezbędny do przywrócenia działania wszystkich systemów, aplikacji i procesów biznesowych [7]. Określając ten parametr, należy

doprowadzić do kompromisu między potencjalnymi stratami a kosztami rozwiązania umożliwiającego najszybsze odtworzenie stanu sprzed awarii.

W przypadku definiowania docelowego punktu odtwarzania systemu do dyspozycji mamy mechanizmy oferowane przez dwie podstawowe technologie [24]:

- tworzenie kopii zapasowych z opcją przenoszenia nośników; przy wykorzystaniu taśm RPO jest rzędu dni, przy wykorzystaniu dysków skraca się natomiast do godzin lub minut;
- replikacja danych, realizowana z wykorzystaniem dysków; przy replikacji możemy uzyskać RPO na poziomie sekund.

W przypadku określania docelowego czasu odtwarzania systemu do wyboru mamy trzy podstawowe rozwiązania [19]:

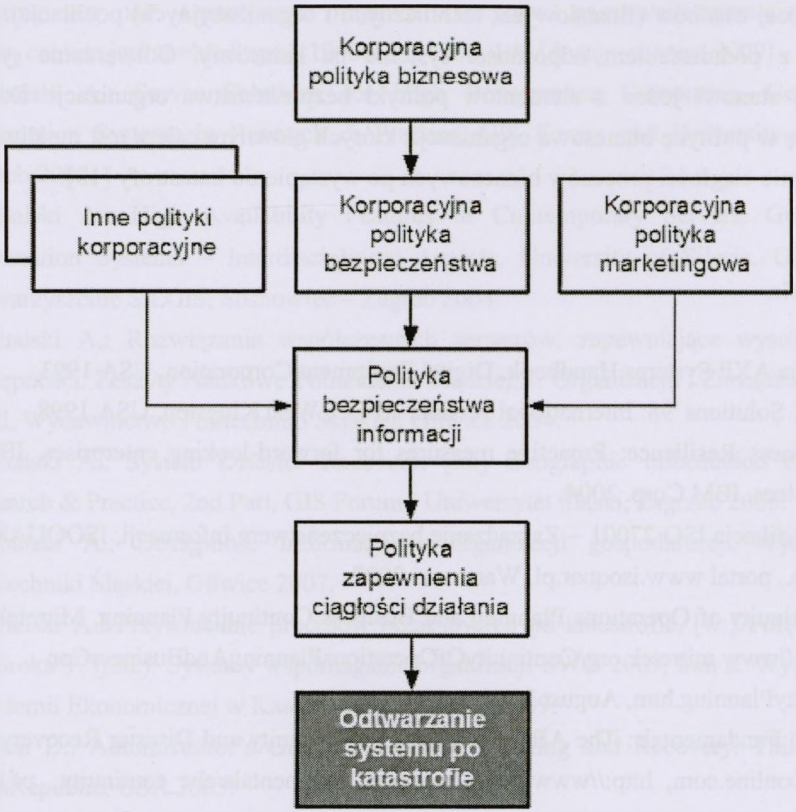
- technologia klastra z mediami dyskowymi [15], pozwalająca na uzyskanie najmniejszych wartości RTO – na poziomie sekund lub minut;
- odtwarzanie z dysków – wówczas RTO jest na poziomie minut lub godzin;
- odtwarzanie z taśm magnetycznych, skutkujące najdłuższym czasem odtwarzania – rzędu godzin lub dni.

Należy także zwrócić uwagę na fakt, że proces odtwarzania danych z taśm lub dysków po katastrofie może zostać radykalnie skrócony przez zastosowanie podejścia zwanego odtwarzaniem „na goły komputer" (ang. *bare metal restore*). Ten żargonowy termin oznacza udostępnienie (w przypadku katastrofy) nowego systemu komputerowego w innym miejscu, na którym następuje odtworzenie aplikacji i danych z nośników zapasowych.

5. Podsumowanie

Zarządzając zasobami informatycznymi organizacji gospodarczej nie jesteśmy w stanie zaplanować przedsięwzięć przeciwdziałających wszelkim możliwym przerwom w pracy systemów. Jednakże podejmowane właściwe działania proaktywne pozwolą uniknąć sytuacji całkowitej utraty danych w przypadku awarii lub katastrofy infrastruktury informatycznej. Podstawą takich działań jest odpowiednie planowanie i przygotowywanie zasobów oraz procedur [12], [26]. Jednakże tylko wkomponowanie tych elementów (związanych z niwelowaniem skutków awarii i wystąpienia katastrofy) w codzienne działania i procedury może zagwarantować, że przedsiębiorstwo jest przygotowane na sytuacje krytyczne.

Zapewnienie ciągłości funkcjonowania organizacji wymaga podejmowania działań dotyczących zarówno sfery technicznej (technologii informatycznych), jak i sfery organizacyjnej (rys. 8).



Rys. 8. Hierarchia polityki działań organizacji [10]
Fig. 8. Hierarchy of the enterprise's policy [10]

W obszarze technologii pierwszy z najistotniejszych czynników to wykorzystanie serwerów opartych na nowoczesnej architekturze, gwarantującej wysoki poziom dostępności mocy obliczeniowej. Drugim elementem są działania związane z tworzeniem zapasowych kopii danych i przechowywaniem ich w geograficznie odległym miejscu, co w połączeniu z usługami kopii bezpieczeństwa (ang. *backup*) chroni przed utratą danych w przypadku katastrofy [21], [25]. Oba wymienione czynniki mają istotny wpływ na organizację i zarządzanie niemal każdej krytycznej aplikacji. Nieodzowne staje się staranne zaplanowanie działań, które powinny być podjęte przed wystąpieniem awarii lub katastrofy i po tym, gdy taka sytuacja miała miejsce [5], [6], [27].

Najwięcej zasobów (finansowych, technicznych i organizacyjnych) pochłaniają działania związane z podniesieniem odporności systemu na katastrofy. Odtwarzanie systemu po katastrofie stanowi jeden z elementów polityki bezpieczeństwa organizacji. Działania te wpisują się w politykę biznesową organizacji, których głównym celem jest możliwie szybkie przywrócenie ciągłości procesów biznesowych po wystąpieniu katastrofy [13].

Bibliografia

1. Alpha AXP Systems Handbook, Digital Equipment Corporation, USA 1993.
2. APC Solutions '98: International version, APCC, West Kingston, USA 1998.
3. Business Resilience: Proactive measures for forward-looking enterprises, IBM Global Services, IBM Corp. 2004.
4. Certyfikacja ISO 27001 – Zarządzanie bezpieczeństwem informacji, ISOQUAR CEE Sp. z o.o., portal www.isoquar.pl, Warszawa 2007.
5. Continuity of Operations Planning and Business Continuity Planning, Mitretek Systems, http://www.mitretek.org/ContinuityOfOperationsPlanningAndBusinessCon tinuityPlanning.htm, August 2006.
6. CSO Fundamentals: The ABCs of Business Continuity and Disaster Recovery Planning, CSOonline.com, http://www.csoonline.com/fundamentals/abc_continuity _pf.html, May 2006.
7. Czym jest odtwarzanie po awarii i co można zrobić w tym zakresie? e-Biuletyn Veritas, issue 1, Veritas Software Corporation, 2004.
8. Florys M.: Awarie struktury IT. Taniej zapobiegać, niż leczyć. Teleinfo, nr 19, Warszawa 2004.
9. How to maximize uptime within existing budget and manpower constraints, The Executive Perspective Series „The Economics of Availability", CMP Media LLC, Custom Media Solutions, USA 2003.
10. Information technology – Security techniques – Management of information and communications technology security, International Standard ISO/IEC 13335-1, 2004.
11. Jakubik K.: Dane zawsze dostępne. NetWorld, nr 3/4, Warszawa 2004.
12. Khosrow-Pour M. (ed.): Advanced Topics in Information Resources Management, Vol. 3, Idea Group Publishing, USA 2003.
13. Liderman K.: Dokumentowanie systemu bezpieczeństwa teleinformatycznego – plan zapewniania ciągłości działania, artykuł opublikowany 3.02.2006 r. na portalu Centrum.Bezpeczeństwa.Pl, http://centrum.bezpieczenstwa.pl/ content/view/292/13 [dostęp: październik 2007].

14. Looking for HP OpenView? https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-10^36657_4000_100 [dostęp: marzec 2009].
15. Michalski A.: Server Solutions for High Performance Computing. Geographical Information Systems in Research & Practice, GIS Forum and University of Silesia, Zagreb 2004.
16. Michalski A.: High Availability Features of Contemporary Servers. Geographical Information Systems – Interdisciplinary Aspects, University of Silesia, GIS Forum, Stowarzyszenie SILGIS, Sosnowiec – Zagreb 2004.
17. Michalski A.: Rozwiązania współczesnych serwerów, zapewniające wysoki poziom dostępności. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, nr 20, cz. II, Wydawnictwo Politechniki Śląskiej, Gliwice 2004.
18. Michalski A.: System Disaster Recovery, [in:] Geographic Information Systems in Research & Practice, 2nd Part, GIS Forum i Uniwersytet Śląski, Zagrzeb 2005.
19. Michalski A.: Dostępność informacji w organizacji gospodarczej. Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
20. Michalski A.: Przywracanie procesów biznesowych po katastrofie, [w:] Porębska-Miąc T., Sroka T. (red.): Systemy wspomagania organizacji SWO 2009, tom 2. Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice 2009.
21. Norton D.: Administrator's Guide to Disaster Planning and Recovery. Third Edition. TechRepublic, USA 2005.
22. Optimize Availability, Compaq Availability Partnership, Compaq Computer Corporation, USA 2001.
23. Schumin B.: Skyline Parkway Motel Burned, zdjęcie w wersji cyfrowej (*.jpg), łącze „A building after arson" w haśle Man-made hazard, wikipedia EN, [dostęp: 13.07.2005].
24. Successful Business Continuity Management and Planning with Veritas Consulting Services, Veritas White Paper „Solving the Business Problem of Downtime", Veritas Software Corporation, 2004.
25. Webster J. and IBM Corp.: Step-by-step Data and Disaster Recovery, IBM Corp. and Illuminata Inc., 2002.
26. When disaster strikes... Will you be ready?, inform Special Insert, Issue 18, July/August 1997, Digital Equipment Corporation, Woburn MA, 1997.
27. Wold G.H.: Disaster Recovery Planning Process. Disaster Recovery Journal, Vol. 5, No. 1 (Part I), No. 2 (Part II) and No. 3 (Part III), 1997.
28. Wołowski F.: Zarządzanie ryzykiem systemów informacyjnych. Materiały XVIII Pełnoletniej Górskiej Szkoły PTI, Szczyrk 2006.

Abstract

The paper deals with the enterprise information security in the case of disaster or system malfunction. There are five chapters in the paper with eight figures in total and the bibliographic source list with 28 entries. In the first chapter role of the information for enterprise activity is discussed (Fig. 1). The second chapter defines system malfunction and disaster states (Fig. 2) and carried out an analysis of main causes of data loss (Figs. 3 and 4). Also three levels of systems' security are specified in this chapter (Fig. 5). The methods preventing data loss in cases of system malfunction and high availability servers are discussed in the third chapter (Fig. 6) and the fourth chapter describes disaster recovery procedures and metrics (Fig. 7). The last chapter highlights the role of the company's security policy and related costs (Fig. 8).